

# RIPE RIS Live!

Jared Mauch

T G I F



**Mirjam (RIPE Labs)**

@mir\_ripe\_labs

Following



We're launching RIS Live, a feed that offers BGP messages in real time. Please give us feedback by filling in the survey. More details on [#RIPELabs: labs.ripe.net/Members/chris\\_](#)

...

# RIPE RIS Launched a demo of live BGP updates

- <https://ris-live.ripe.net>
- Launched Feb 15th
  - [https://labs.ripe.net/Members/chris\\_amin/ris-live-bgp-message-stream](https://labs.ripe.net/Members/chris_amin/ris-live-bgp-message-stream)

“We are launching a prototype called RIS Live, a feed that offers BGP messages in real time. It collects information from the RIS Route Collectors (RRCs) and uses a WebSocket JSON API to monitor and detect routing events around the world.”

- Important as it has a decent number of views
- Realtime!
  - No more cron/fetching files
- Trial ENDS August 2019

# It's still experimental

- RIPE says it's measuring interest in this
- It's a prototype
- I think it's super valuable
- I think you should say so too
- I think we should have other public route collection systems move to real time
- I think you should be sending a BGP feed to RIS as well
  - [Invisible Hijacking - RIPE 72](#)
  - [https://ripe72.ripe.net/presentations/45-Invisible\\_Hijacking.pdf](https://ripe72.ripe.net/presentations/45-Invisible_Hijacking.pdf)

# Selective

- Can match on useful things
  - Prefix
  - AS\_PATH
  - UPDATE Messages
  - Announcements or Withdraws
  - More Specific Route or Less Specific routes
  - Specific collectors
  - Can get the raw BGP messages as well

# Making it happen

- Easy!
  - Less than 60 lines of python3 code builds you a route monitoring system
  - Including radix tree lookups
    - Find those pesky more-specific leaks
    - Or hijacks
  - Load in customer prefixes
- It's so easy I did it in under an hour!
- Make it report to your shared space (Slack, WebEx Teams, etc)

# Upgrading route leak monitoring

- NANOG 41 - [Detecting Routing Leaks by Counting](#)
- Been fetching MRT files from route-views since 2007 for finding BGP filtering issues
  - <https://puck.nether.net/bgp/leakinfo.cgi>
- Watches for AS\_PATHs with too many “tier1” ASNs in the path
- Limited view of what goes into route-views
- RIPE RIS has more views
- Can subscribe to just AS\_PATHs I care about
  - Makes the data consumption problem much easier
  - Immediate feedback of odd events is better

# Some early results

2402:28c0:fffc::/48

47950 62184 3257 4134 36678 4809 1299 174 136620 137413

2a07:a905:ff10::/48

8455 3257 4134 36678 4809 1299 174 136620 137413

168.133.52.0/22

5511 7922 7016 30070 3549

# Some software that can use this already

- <https://github.com/jaredmauch/rislive>
  - This is my fault (features/pr welcome)
- <https://github.com/nlnog/bgpalerter>
  - Self-hosted route monitoring and alerting
- Other important software/links
  - [ARTEMIS](#)

Questions?

Jared Mauch

jared@puck.nether.net

@jaredmauch